Linux Network Servers

OpenLDAP

A cada dia que surgem novos sistemas nas empresas a fim de resolver diversos tipos de problemas, logo cresce a necessidade de ter um maior controle e melhores mecanismos de busca de informação. Segurança e controle de dados são imprescindíveis em qualquer empresa. Umas das vantagens do OpenLdap é a possibilidade de que vários sistemas possam compartilhar de base de dados de usuários e senhas de forma centralizada e integrada.

O projeto OpenLdap é um serviço de diretório, que utiliza o protoloco LDAP (Lightweight Directory Access Protocol – Protocolo Leve de Acesso a Diretórios), baseado no protocolo X.500. O OpenLdap utiliza o trafego de dados via TCP-IP podendo ser implementado em diversas plataformas em redes IPV4 e IPV6, possibilitando autenticação, mecanismos de segurança no uso de certificados e criptografia, podendo ser configurado para restringir acesso a socket layer, ter multipla instâncias de banco de dados, múltiplas Threads, permite replicação e configuração do serviço de acordo com a sua necessidade através de Schema.

Características de um sistema de diretórios

- Centraliza e organiza informações;
- Evita redundância;
- É otimizado para fazer pesquisas, pois utiliza algoritmos de busca sofisticados;
- Podem ser distribuídos, isto é, não precisam necessariamente armazenar suas informações em um mesmo local.

Estrutura do LDAP

A organização da estrutura de dados do OpenLdap é hierárquica, sendo referenciada a forma de Árvore, com conceito de orientação de objetos. A árvore de informações do LDAP possui um elemento raiz, onde começa a busca das informações. Sendo assim, o sistema percorre os nós filhos até encontrar o elemento desejado. A raiz e seus ramos são diretórios. Por exemplo: temos um diretório raiz, depois temos a rede da empresa, o departamento (diretoria, secretaria, financeiro etc) e o funcionário. Logo, um diretório pode ter seus sub-diretórios que são chamados de entradas. Cada entrada possui um ou mais atributos (características). Os diretórios representam a raiz e os ramos, as entradas representam as folhas.

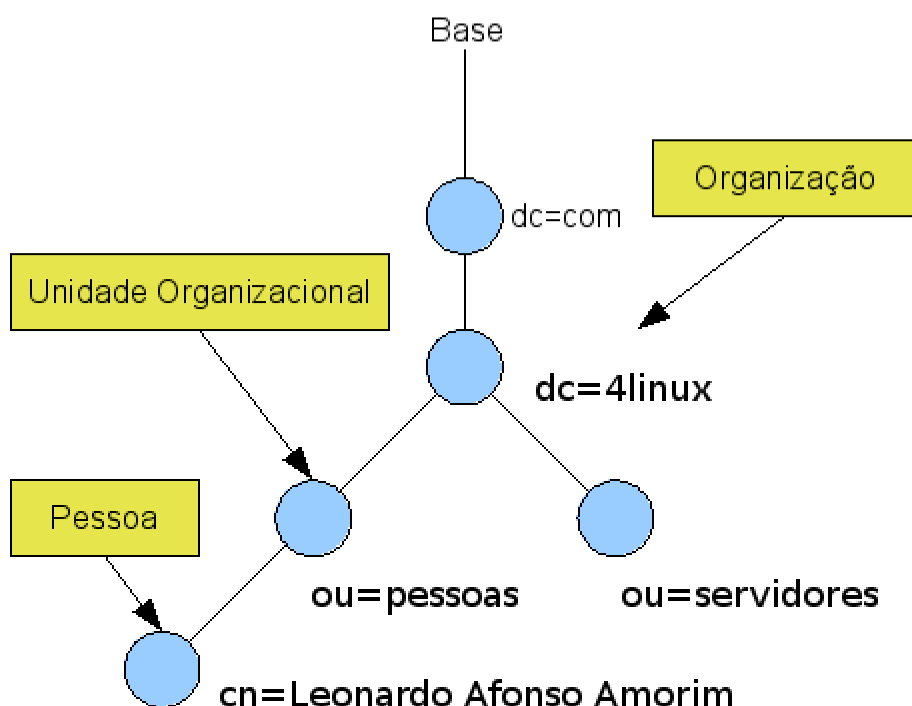
Atributos de diretórios:

Atributo	Descrição
c	Representa país (country)
o	Representa uma ornanização como uma empresa (organization)
ou	Representa um departamento (organization unit)

Linux Network Servers

Atributos de entradas:

Atributo	**Descrição**
cn	Representa um nome (common name)
uid	Representa a identidade de um usuário (user ID)
gn	Representa o nome próprio de uma pessoa (given name)
sn	Representa o sobrenome de uma pessoa (surname)



OpenLdap constitui-se de:

slapd - serviço openldap;
slurpd - serviço para replicação e atualização openldap;
libraries - são bibliotecas para implementação do OpenLdap, com utilitários e ferramentas;

Linux Network Servers

O arquivo de configuração do OpenLDAP é (no Debian):

```
/etc/ldap/sldap.conf
```

Em outras distribuições, o arquivo pode ser encontrado em:

```
/usr/local/etc/openldap/slapd.conf
```

Instale pacotes do OpenLdap:

```
# aptitude install libldap2 ldap-utils slapd
```

Configure as opções do OpenLdap:

```
# dpkg-reconfigure slapd
```

Configure quando for solicitado em:

Omitir configuração do servidor OpenLdap: NÃO
Informe o nome de domínio DNS para construir a base dn: seunome.com.br
Informe nome da organização: 4linux
Digite senha: 123456
Escolha base de dados: BDB
Remoção da base de dados quando o pacote slapd for expurgado: NÃO
Mover base antiga de dados em /var/lib/ldap: SIM
Permitir protocolo LDAPv2: SIM (Requirido para integrar o Squid com OpenLDAP)

Inicie o serviço do OpenLdap:

```
# /etc/init.d/slapd start
```

OBS: Você poderá iniciar o serviço do OpenLdap em algumas distribuições com /usr/local/libexec/slapd

Verifique se o serviço está disponível para a rede:

```
# netstat -lp | grep ldap
```

Visualize a base física de dados do OpenLDAP:

```
# ls /var/lib/ldap/
```

Linux Network Servers

Visualize o arquivo de configuração OpenLDAP no Debian:

OBS: Em algumas distribuições o arquivo de configuração pode estar em /usr/local/etc/openldap/slapd.conf

```
# vi /etc/ldap/slapd.conf
```

```
# Este é o principal arquivo de configuração do slapd. Veja man page slapd.conf
# para verificar demais configurações

#########################################################################

# Configurações Globais

# Autorizar LDAPv2 binds
allow bind_v2

# Definições de Schema e objectClass
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

# Local do arquivo onde encontra o número do processo slapd.
O script init.d nãi parará o servidor se você mudar isto.
pidfile         /var/run/slapd/slapd.pid

# Lista de argumentos a serem passados para o servidor
argsfile        /var/run/slapd/slapd.args
```

Linux Network Servers

```
# Nível de logs a serem gerados pelo servidor, leia slapd.conf para maiores
# informações
loglevel        0

# Local onde módulos diâmicos são armazenados
modulepath    /usr/lib/ldap
moduleload    back_bdb

#Verificação de schema
schemacheck      on

# O número máximo de entradas que estão retornadas para operação de busca
sizelimit 500

# Parâmetros para configuração de Threads / CPU
tool-threads 1

##########################################################
#############
# Especificação de Diretivas para o bdb
# 'backend' directive occurs
backend                 bdb
checkpoint 512 30

##########################################################
#############
#  Especificação de Diretivas para outro:
# 'backend' directive occurs
#backend                <other>

##########################################################
#############
```

Linux Network Servers

```
# Especificação de diretivas para banco de dados #1, tipo bdb:
# 'database' directive occurs
database        bdb

# Definição de sufixo da base
suffix          "dc=teste,dc=seu-nome,dc=br"

# rootdn diretiva para especificar um super usuário no banco de dados.
# Isto é preciso.
# for syncrepl.
# rootdn          "cn=admin,dc=teste,dc=seu-nome,dc=br"

# Local onde os arquivos de banco de dados são armazenados fisicamente #1
directory       "/var/lib/ldap"

# Para pacote Debian, não usamos 2MB como default mas tenha certeza de atualizar
# este valor
dbconfig set_cachesize 0 2097152 0

# Verificar informações de bugs encontrados nestes parâmetros
# http://bugs.debian.org/303057

# Números de objetos que podem ser travados no mesmo tempo
dbconfig set_lk_max_objects 1500
#Números de lockers (ambas requisições e concessões)
dbconfig set_lk_max_locks 1500
#Números de lockers
dbconfig set_lk_max_lockers 1500

# Opções de indexação #1
index           objectClass eq
```

Linux Network Servers

```
# Salva o tempo que entradas foram modificadas no banco de dados
lastmod         on

# Local onde são replicados os logs do banco de dados
# replogfile    /var/lib/ldap/replog

# Parâmetros de acesso e permissões
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=teste,dc=seu-nome,dc=br" write
        by anonymous auth
        by self write
        by * none
access to dn.base="" by * read

        by dn="cn=admin,dc=teste,dc=seu-nome,dc=br" write
        by * read
#access to dn=".*,ou=Roaming,o=morsnet"
#        by dn="cn=admin,dc=teste,dc=seu-nome,dc=br" write
#        by dnattr=owner write
# Especificação de diretivas de banco de dados #2, de tipo outro, pode
ser bdb:
# 'database' directive occurs
#database        <other>
# Definição de sufixo da base#2
#suffix          "dc=debian,dc=org"

##########################################################################
```

Linux Network Servers

Verificação de teste da configuração do arquivo do OpenLdap:

```
# slaptest
```

É necessário criar a nossa base de dados. Para tal utilizaremos **migrationtools**, uma ferramenta para migração de base de dados escrita em Perl para o OpenLdap. Portanto verifique e instale os pacote migrationtools e perl:

Verifique se tem o pacote perl instalado:

```
# dpkg -l | grep perl
```

Instale Perl, caso não esteja instalado:

```
# aptitude install perl
```

Verifique o pacote Migration Tools:

```
# aptitude search migrationtools
```

Realize a instalação Migration Tools:

```
# aptitude install migrationtools
```

Acesse o diretório /usr/share/migrationtools e copie o arquivo de configuração:

```
# cd /usr/share/migrationtools
# cp -av migrate_common.ph  migrate_common.ph.original
```

Edite o arquivo migrate_common.ph e os campos a seguir, salve:

```
$DEFAULT_MAIL_DOMAIN="[seu-nome].com.br";
$DEFAULT_BASE=dc="[seu-nome],dc=com,dc=br";
```

Vamos migrar a base de usuários do sistema (/etc/passwd) para uma base padrão LDIF, para inserir na base LDAP:

```
# cd /usr/share/migrationtools
# ./migrate_passwd.pl /etc/passwd /etc/ldap/users.ldif
```

Linux Network Servers

Verifique o arquivo /etc/ldap/users.ldif criado e observe o conteúdo:

```
# less /etc/ldap/users.ldif

gidNumber: 106
homeDirectory: /var/lib/gdm
gecos: Gnome Display Manager

dn: uid=root,ou=People,dc=[seu-nome],dc=com,dc=br
uid: root
cn:: cm9vdA==
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$dL7nEggA$P6Ib/H9QBkdd/sTcUBW1z1
shadowLastChange: 12495
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 0
gidNumber: 0
homeDirectory: /root
gecos: root
```

Agora vamos migrar a base de grupos do sistema (/etc/group) para uma base padrão LDIF, para inserir na base LDAP:

```
./migrate_group.pl /etc/group /etc/ldap/groups.ldif
```

Verifique os arquivos gerados em /etc/ldap/group.ldif:

```
# cat /etc/ldap/groups.ldif
```

Linux Network Servers

Crie base ldif:

```
# ./migrate_base.pl > /etc/ldap/base.ldif
```

Edite o arquivo gerado em /etc/ldap/base.ldif e remova as linhas de 1 a 9, por default durante a migração estas linhas foram criadas, podendo gerar erro durante a importação:

```
# vi /etc/ldap/base.ldif
```

Adicione o base ldif na base do OpenLDAP:

```
# ldapadd -x -D cn=admin,dc=seunome,dc=com,dc=br -f /etc/ldap/base.ldif -W
```

Parâmetros do comando ldapadd:

-f = especifica o arquivo que será incluído

-D = especifica o domínio
-W = chama um prompt para digitar a senha

Realize uma busca na sua base de dados OpenLdap:

```
# ldapsearch -x | more
```

Parâmetros do comando ldapsearch:
-x = utiliza autenticação simples

Adicione o group.ldif:

```
# ldapadd -x -D cn=admin,dc=[seu-nome],dc=com,dc=br -f /etc/ldap/group.ldif -W
```

Adicione o user.ldif:

```
# ldapadd -x -D cn=admin,dc=[seu-nome],dc=com,dc=br -f /etc/ldap/users.ldif -W
```

Você pode transferir as informações em formato ldif através do slapadd passando a informação direto para servidor:

```
# /etc/init.d/slapd stop
```

```
# slapadd -l meuarquivo.ldif -f slapd.conf
```



Linux Network Servers

Realizando busca específica através do nome do objeto que consta na base do OpenLdap:

```
# ldapsearch -x -b 'dc=seunome,dc=com,dc=br' '(cn=cdrom)'
```

Parâmetros do comando ldapsearch:
-x = utiliza autenticação simples
-b = diretório onde será feita a busca

Consulta da Base OpenLdap:

```
# slapcat | more
```

Configuração do Cliente Ldap

Vamos configurar o cliente ldap:

```
# vi /etc/ldap/ldap.conf
```

Inclua as seguintes informações:

```
hostname 127.0.0.1
base dc=seunome,dc=com,dc=br
pam_password md5
pam_filter objectclass=account
pam_groupdn cn=users,ou=Group,dc=seunome,dc=com,dc=br
```

Linux Network Servers

Acessando o OpenLdap via Browser com PhpLdapAdmin

Vamos acessar a base do OpenLdap via Browser, para tal será necessário instalar php e dar suporte ao Apache. Instale os pacotes do php necessários para o OpenLdap:

```
# aptitude install php-pear php5-ldap
```

Verifique se seu servidor Apache está com suporte a PHP:

```
# ls -l /etc/apache2/mods-enable
```

Instalando os pacotes do phpldapadmin:

```
# aptitude install phpldapadmin
```

Abra o seu browser e digite no campo URL:

```
127.0.0.1/phpldapadmin/index.html
```

Autenticando o Squid na base de usuários LDAP

No nosso caso, queremos que os usuários do nosso servidor OpenLDAP sejam autenticados. Para isso, usaremos o programa ldap_auth.

Modifique as seguintes linhas no arquivo /etc/squid/squid.conf para ser feita a autenticação via OpenLDAP:

```
# vi /etc/squid/squid.conf

auth_param basic program /usr/lib/squid/ldap_auth -b dc=[seu-nome],dc=com,dc=br -f uid=
%s 192.168.0.124
```

OBS: Não esquecer de tirar a outra linha de autenticação usando ncsa.